

# Perancangan Kriptografi *Block Cipher* Berbasis Pada Teknik Lipat Amplop dan *Linear Congruential Generator* (LCG)

<sup>1</sup>Aprilio Luhukay, <sup>2</sup>Hindriyanto D. Purnomo, <sup>3</sup>Alz Danny Wowor

Fakultas Teknologi Informasi

Universitas Kristen Satya Wacana

Jl. Diponegoro 52-60, Salatiga 50711, Indonesia

Email: <sup>1</sup>apriliohukay@gmail.com, <sup>2</sup>hindriyanto.purnomo@staff.uksw.edu,

<sup>3</sup>alzdanny.wowor@staff.uksw.edu

## Abstract

*Cryptography has a very important role in the security of the data or information. However there is a lot of cryptography which has been solved by cryptanalyst, therefore it is necessary to design a new cryptography as substitute algorithm has been solved. This research designs a Block Cipher cryptography using the flip envelop technique and the Linear Congruential Generator (LCG) were created as a generate key, then the encryption and decryption process designed in four iteration to get a ciphertext and plaintext after using XOR with the key that has been regenerated. The result of this research can be used as an alternative for data security and also as new cryptography.*

**Keywords :** *Cryptography, Cryptanalysis, Block Cipher, Technique Flip Envelope, ASCII*

## Abstrak

Kriptografi sangat berperan dalam keamanan suatu data atau informasi. Namun, banyak kriptografi yang telah dipecahkan oleh kriptanalis, oleh karena itu perlu adanya perancangan algoritma kriptografi baru sebagai pengganti algoritma yang sudah terpecahkan. Penelitian ini merancang sebuah kriptografi *Block Cipher* menggunakan teknik lipat amplop dan *linear congruential generator* (LCG) sebagai pembangkit kunci, kemudian proses enkripsi dan dekripsi dirancang sebanyak empat putaran untuk mendapatkan *ciphertext* dan *plaintext* setelah di-XOR dengan kunci yang sudah diregenerasi. Hasil dari penelitian ini dapat digunakan sebagai alternatif pengamanan data dan juga sebagai teknik kriptografi baru.

**Kata Kunci :** Kriptografi, Kriptanalis, *Block Cipher*, Teknik Lipat Amplop, LCG

---

<sup>1</sup> Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi Universitas Kristen Satya Wacana, Salatiga.

<sup>2</sup> Staff pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.

<sup>3</sup> Staff pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.